LES PROGRAMMES MALVEILLANTS (MALWARE)



1- TYPES D'ATTAQUES

- Pour protéger convenablement les ordinateurs et le réseau, vous devez comprendre ces deux types de menaces contre la sécurité informatique :
  - **Menaces physiques** : événements ou attaques visant à voler, à endommager ou à détruire des équipements tels que les serveurs, les commutateurs et le câblage.
  - **Menaces contre les données** : événements ou attaques visant à supprimer, endommager ou voler des informations, à permettre leur utilisation par des personnes non autorisées ou à en interdire l'accès aux personnes autorisées.

2- MALWARE

- Les ordinateurs et les données qu'ils contiennent doivent être protégés contre les programmes malveillants :
  - **Les programmes malveillants (malwares)** sont conçus pour nuire à un système. Le terme malware est une abréviation de **mal**icious soft**ware**.
  - Ces programmes s'installent généralement sur l'ordinateur à l'insu de l'utilisateur. Ils peuvent ouvrir des fenêtres indésirables ou modifier la configuration.
  - Ils sont également capables de modifier les navigateurs Web pour rediriger l'utilisateur vers des pages indésirables. Ce procédé s'appelle la redirection.
  - Ils peuvent aussi récupérer certaines informations stockées sur l'ordinateur à l'insu de l'utilisateur.
  - Ils peuvent être utilisé pour prendre le contrôle d'un ordinateur à distance.

2.1 MALWARE - VIRUS

- Le premier type de programme malveillant, et le plus répandu, est **le virus informatique.** Il se transmet entre ordinateurs via les e-mails, les lecteurs USB, les transferts de fichiers et la messagerie instantanée.
- Le virus est **caché dans du code**, **un logiciel** **ou** **des documents**.
- Lorsque l'utilisateur accède au fichier en question, le virus s'exécute et contamine l'ordinateur.

Les virus peuvent...

- Modifier, endommager, supprimer les fichiers, voire effacer tout le contenu d'un disque dur sur l'ordinateur.
- Empêcher l'ordinateur de démarrer, faire que les applications ne se chargent pas ou ne fonctionnent pas correctement.
- Utiliser le compte de messagerie des utilisateurs pour répandre le virus sur d'autres ordinateurs.
- Rester inactifs jusqu'à ce qu'ils soient appelés par le pirate.
- Enregistrer la frappe et capturer des informations sensibles, comme des mots de passe et/ou des numéros de carte de crédit et envoyer ces données au pirate.

2-2 MALWARE – VER (WORM)

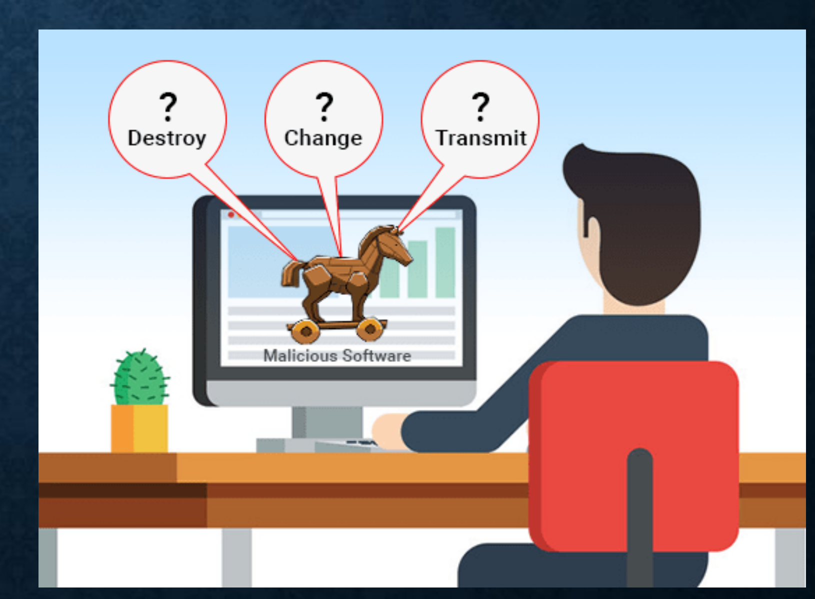
- En informatique un ver est un programme qui diffère des virus par plusieurs points.
- Tout d'abord le **ver** est **un programme autonome**, qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet, contrairement aux virus qui infectent les fichiers et leur code exécutable.
- Il se propage sur un réseau pour infecter un maximum de systèmes.
- Le ver est employé pour réaliser une attaque par déni de service. C'est-à-dire qu'il sature un réseau ou un site Web ciblé afin pour le rendre inaccessible.
- La propagation d'un ver informatique intervient essentiellement dans le cadre d'une pièce jointe attachée a un courriel, de la navigation sur des forums et des sites non sécurisés ou eux-mêmes infectés.



Regardez: **Vidéo Computer Worm**

2-3 MALWARE - CHEVAL DE TROIE (TROJAN)

- **Le cheval de Troie** se présente **comme un programme utile**, mais il contient du code malveillant. Par exemple, ils sont souvent dissimulés dans les jeux en ligne gratuits. Ces jeux sont téléchargés sur l'ordinateur, mais ils contiennent également un cheval de Troie.
- Pendant que l'utilisateur joue, le cheval de Troie s'installe sur le système et continue de fonctionner, même une fois le jeu fermé.
- Une fois activés, les chevaux de Troie peuvent permettre aux cybercriminels de vous espionner, de dérober vos données sensibles et **d'accéder à votre système à distance** à l'aide d'un backdoor (porte dérobée).
- Ces actions peuvent être les suivantes :
  - Blocage et suppression de données.
  - Copie et modification de données.
  - Perturbation des performances des ordinateurs ou des réseaux informatiques.



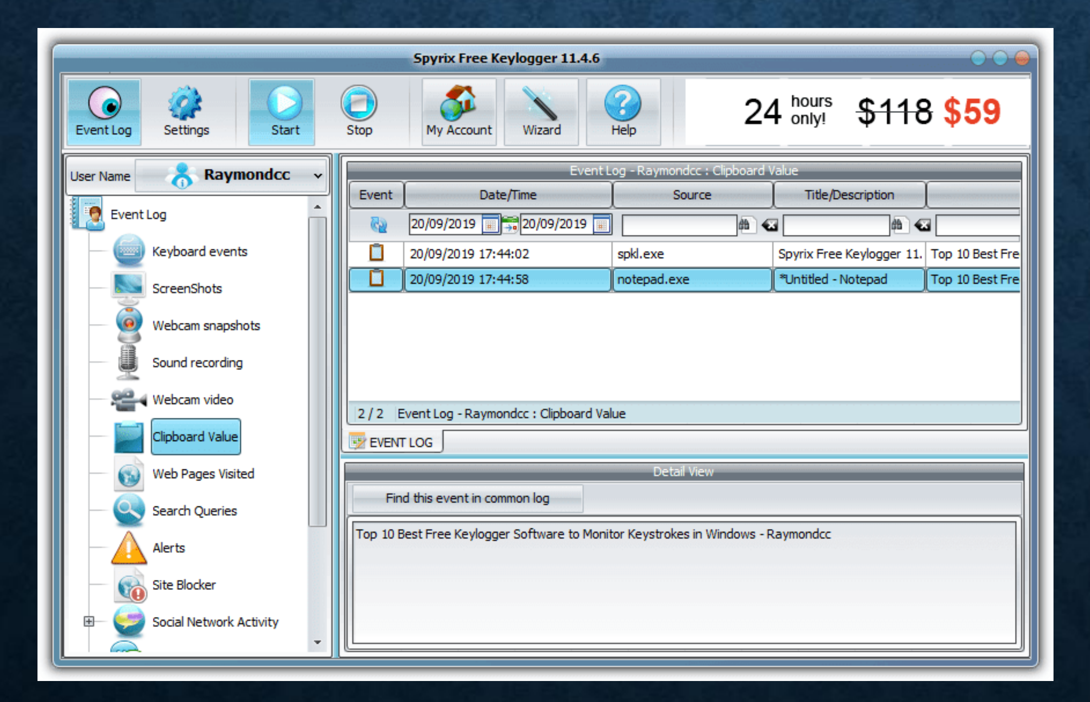
2-4 MALWARE – LOGICIEL ESPION (SPYWARE)

- Contraction des mots anglais *spy* (« espion ») et *software* (« logiciel »), le terme «spyware » désigne un logiciel espion qui collecte des données personnelles afin de les envoyer à un tiers.
- Ce type de programme malveillant est la plupart du temps caché dans des logiciels gratuits ou des mises à jour de sécurité, mais il peut aussi se propager depuis une page Internet infectée.
- L'installation du logiciel espion se fait à l'insu de la victime. Une fois en place, il va enregistrer différents types de données selon sa vocation : adresses des sites Web visités, requêtes tapées dans les moteurs de recherche, données personnelles (nom, adresse de courrier électronique, coordonnées…), type de produits achetés en ligne.
- Certains peuvent dérober des informations bancaires. Ces informations sont exploitées à des fins de **profilage pour l'envoi de publicités ciblées** sur les centres d'intérêt de la personne qui a été espionnée.

EXEMPLE DE SPYAWRE : KEYLOGGER

- Un **keylogger** est un type de spyware spécialisé pour **espionner les frappes au clavier** sur l'ordinateur qui l'héberge, et pour les transmettre via internet à une adresse où un pirate pourra les exploiter.
- Un keylogger peut donc recueillir et transmettre vos mots de passe, code de carte bancaire, intitulé sous lequel vous ouvrez une session…

https://www.raymond.cc/blog/free-and-simple-keylogger-to-monitor-keystrokes-in-windows/



2-4 MALWARE – LOGICIEL PUBLICITAIRE (ADWARE)

- Le terme « adware » est une contraction des mots anglais *advertising* et *software* que l'on traduit par « logiciel publicitaire » ou encore « publiciel ».
- Il s'agit d'un programme informatique qui affiche des publicités sur l'interface d'un logiciel ou via le navigateur Internet sous forme de **fenêtres pop-up** qui jaillissent de façon chronique.
- Dans la plupart des cas, l'adware est intégré à un logiciel gratuit ou un courriel indésirable.
- Bien que n'étant pas dangereux pour l'ordinateur, l'adware est considéré comme un logiciel malveillant (malware) par son fonctionnement agressif et dérangeant.
- Il affecte aussi la performance de l'ordinateur.



2-5 MALWARE – RANÇONGICIEL (RANSOMWARE)

- C'est un logiciel informatique malveillant, **prenant en otage les données.**
- Le ransomware chiffre et bloque les fichiers contenus sur votre ordinateur et demande une rançon (de l'argent) en échange d'une clé permettant de les déchiffrer.
- Apparus dans un premier temps en Russie, les ransomwares se sont répandus dans le monde entier, et principalement aux Etats-Unis, en Australie ou en Allemagne.
- La seule solution est de payer la rançon ou restaurer vos données à partir d'un sauvegarde (backup).



Alerte de sécurité : Recrudescence des rançongiciels

DD Direction des technologies de l'information <ccti-communication@cmontmorency.qc.ca>
À Tohmé, Antoine

Répondre | Répondre à tous

En cas de problème lié à l'affichage de ce message, cliquez ici pour l'afficher dans un navigateur web.

ALERTE DE SÉCURITÉ



RECRUDESCENCE DE LA MENACE DES RANÇONGICIELS !

ATTENTION ! Des organismes publics sont actuellement la cible d'une campagne de rançongiciel. Les rançongiciels peuvent entrainer de graves impacts informatiques tels que la perte de données corporatives et personnelles, le blocage du matériel informatique comme votre poste de travail et même l'infection des serveurs auxquels vous avez accès !

Comment éviter de se faire prendre ?

Données personnelles :

- Faites des sauvegardes sur un support externe régulièrement;
  - Utilisez un support externe (ex. : Clé USB, disque externe, DVD);
- Assurez-vous de faire les mises à jour de sécurité sur vos appareils personnels
  - Le système d'exploitation et vos logiciels;
  - Vos données peuvent infecter d'autres systèmes lorsqu'elles transitent sur d'autres réseaux. Gardez tous vos appareils à jour.

Données professionnelles :

- Sauvegardez vos documents dans les espaces réseau dédiés à cette fin plutôt que sur votre poste;
- Avisez le CCTI+ de tout comportement suspect IMMÉDIATEMENT;
- Évitez de connecter les appareils du collège sur des réseaux publics.
- Évitez d'utiliser les appareils du collège pour naviguer sur des sites qui ne sont pas en lien avec la mission du collège.

2-6 MALWARE – HAMEÇONNAGE (PHISHING)

- **L'hameçonnage** est un stratagème de fraude qui consiste à envoyer massivement des courriels ou des textos semblant provenir d'une institution financière, comme une banque, ou d'une entreprise connue.
- Le pirate peut demander des informations pour vérification, par exemple le nom d'utilisateur, le mot de passe ou le code PIN, la plupart du temps pour « protéger l'utilisateur ou éviter des événements désastreux ». Si l'utilisateur fournit les informations demandées, l'attaque d'hameçonnage a réussi.
- Les conséquences potentielles de ce type d'attaque peuvent s'avérer importantes : perte de vos données, accès non autorisés ou vol de vos informations confidentielles dans le but de commettre des fraudes.



Alerte de sécurité : le réseau de l'enseignement supérieur visé par des campagnes d'hameçonnage

DD Direction des technologies de l'information <directionti@cmontmorency.qc.ca>
À Tohmé, Antoine

Répondre | Répondre à tous

En cas de problème lié à l'affichage de ce message, cliquez ici pour l'afficher dans un navigateur web.

ALERTE DE SÉCURITÉ



LE RÉSEAU DE L'ÉDUCATION VISÉ PAR UNE CAMPAGNE D'HAMEÇONNAGE

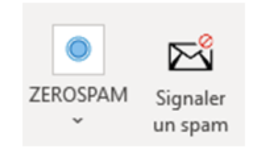
En effet, une campagne d'hameçonnage, visant à distribuer le logiciel malveillant "*Emotet*" a ciblé deux établissements de notre réseau de l'éducation au cours des deux dernières semaines. (Consultez la section "Que faire si vous recevez ce type de courriel ci-dessous.)

Que faire si vous recevez ce type de courriel?

Si vous recevez ce type de courriel, SURTOUT NE L'OUVREZ PAS!

Dans l'application Outlook locale:

1. Assurez-vous que le courriel suspect soit en surbrillance (c'est-à-dire sélectionné)
2. Dans le coin supérieur droit, repérez l'une des deux icônes ci-dessous:
3. Cliquez sur l'icône.

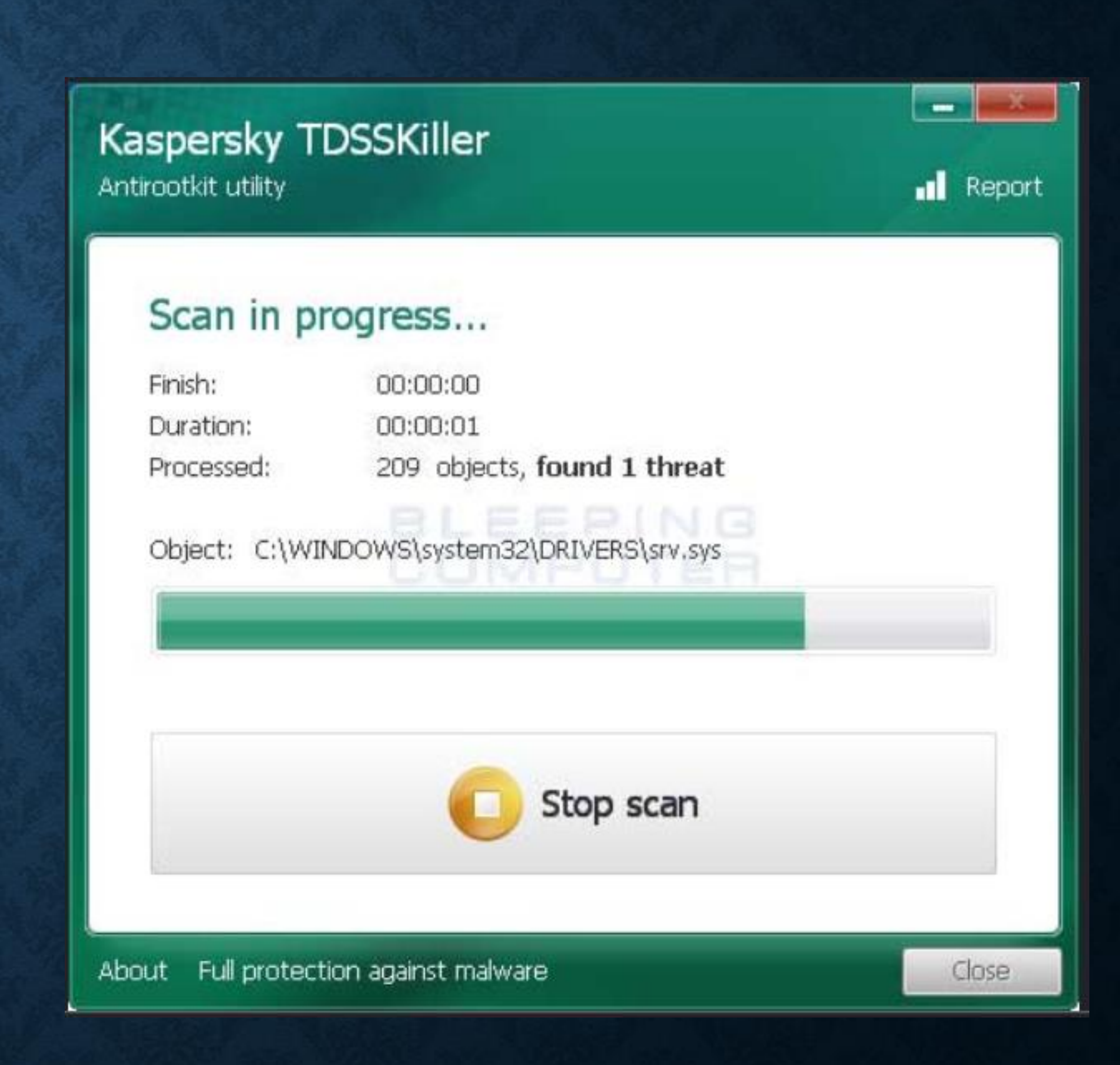


Dans l'application Outlook Web:

1. Assurez-vous que le courriel suspect soit en surbrillance (c'est-à dire sélectionné)
2. Dans le coin supérieur droit, repérer les "…" et cliquez dessus
3. Dans le menu déroulant, sélectionnez "Option de sécurité", "Marquer comme hameçonnage".

2-7 MALWARE – ROOTKITS

- Un rootkit est un terme anglais qui désigne un type de malware conçu pour infecter un PC et qui permet au pirate d'installer une série d'outils qui lui permettent d'accéder à distance à un ordinateur.
- Le malware sera habituellement bien **caché dans le système d'exploitation** et ne **sera pas détecté par les logiciels anti-virus** et autres outils de sécurité.
- Un logiciel spécial de suppression des rootkits est utilisé, tels que **TDSSKiller,** mais parfois, la réinstallation du système d'exploitation est nécessaire pour garantir la suppression totale du rootkit.
  https://usa.kaspersky.com/downloads/tdsskiller

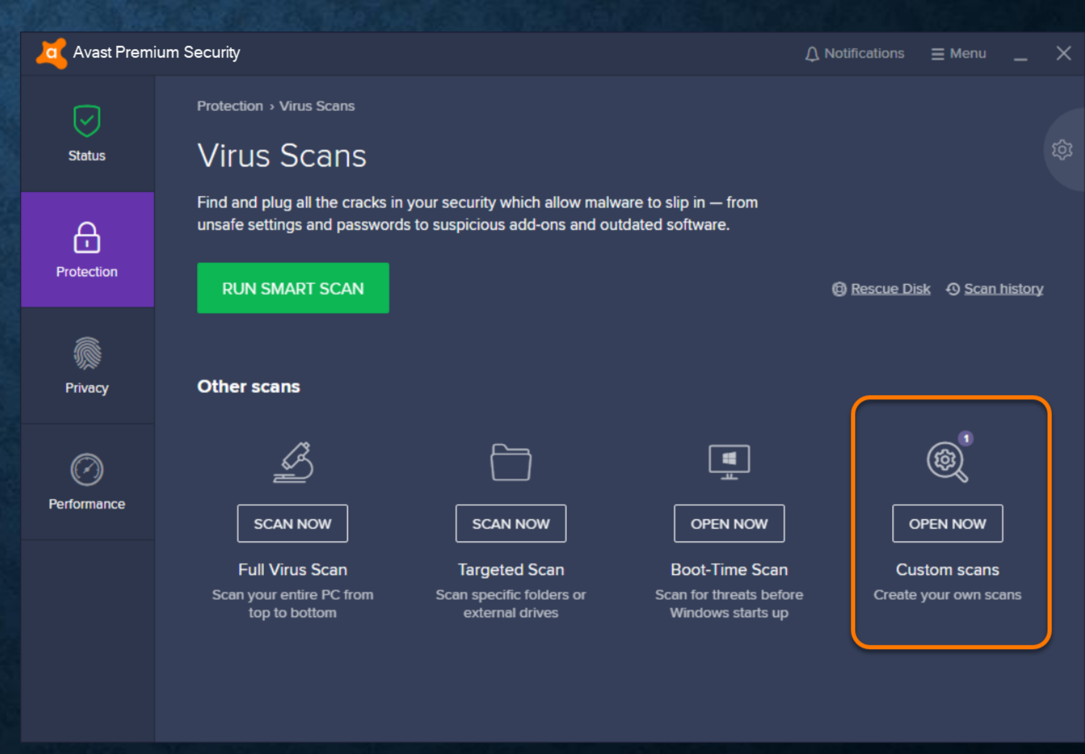


3- COMBATTRE LES MALWARE

- Les programmes malveillants (Malware) peuvent être des virus, des vers, des chevaux de Troie, des logiciels espions (ex: des enregistreurs de frappe) ou des logiciels publicitaires.
- Ils sont conçus pour s'immiscer dans la vie privée, voler des informations, endommager le système ou supprimer des données endommagées.
- Il est important que vous protégez les ordinateurs et les appareils mobiles à l'aide d'un logiciel anti-programme malveillant.

- **Protection antivirus :** le programme surveille en permanence les virus. Lorsqu'un virus est détecté, l'utilisateur est averti et le programme tente de mettre le virus en quarantaine ou de le supprimer.

- **Protection contre les Worms:** Mettre à jour les systèmes et leurs failles de sécurité.

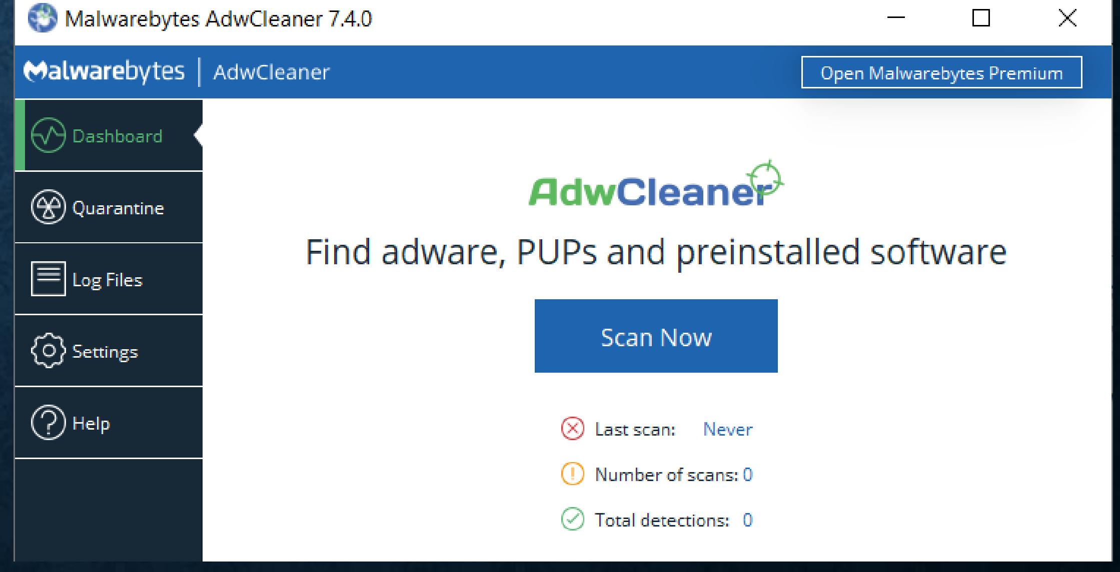


COMBATTRE LES MALWARE

- **Protection contre les logiciels espions (anti-spyware)** : ce programme recherche les enregistreurs de frappe (keyloggers) et autres logiciels espions (spywares).

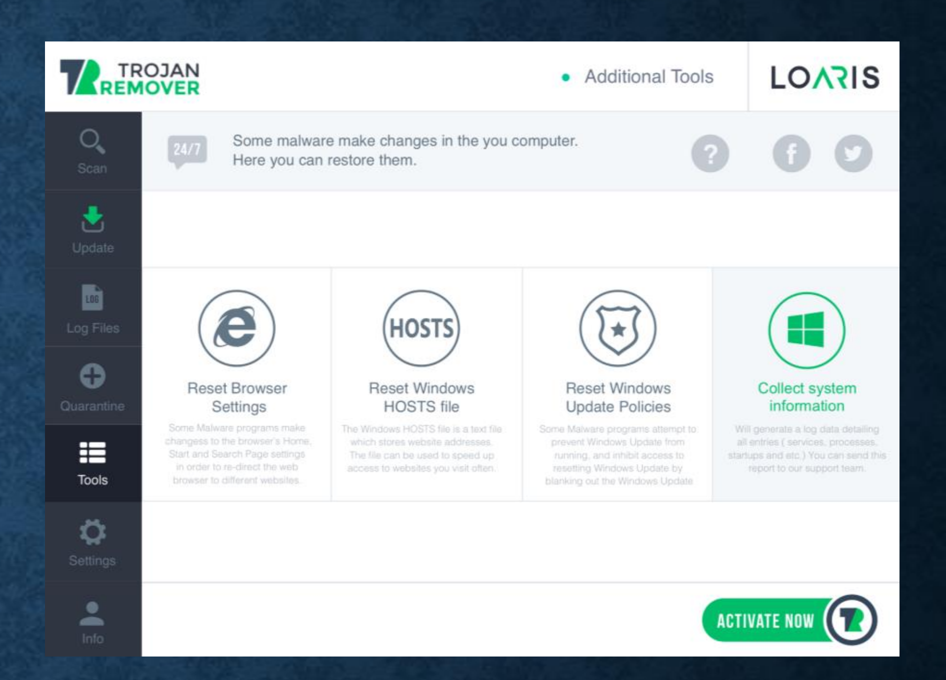


- **Protection contre les logiciels publicitaires (anti-adware)** : ce programme recherche les programmes qui affichent de la publicité sur votre ordinateur.

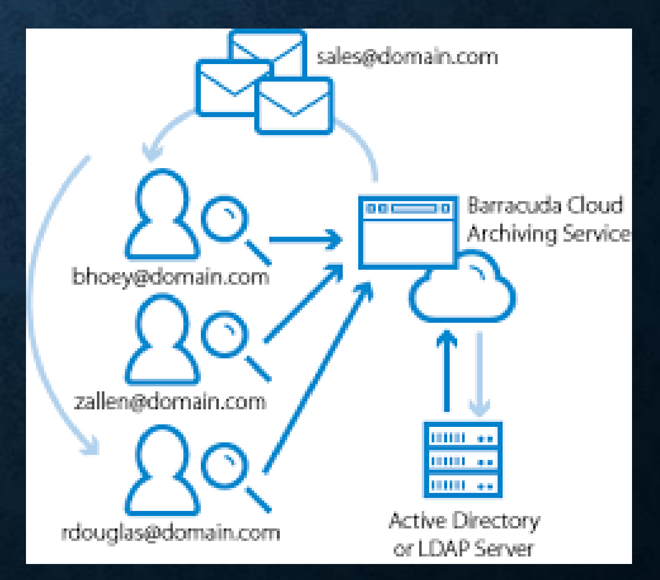


COMBATTRE LES MALWARE

- **Protection contre les cheval à troie (Trojan Remover):** ce programme permette de détecter et de supprimer des logiciels malveillants notamment le cheval de Troie. Il supporte le scan personnalisé et possède une base de données mis à jour régulièrement.



- **Protection contre l'hameçonnage (Anti-Phishing):** ce programme bloque les adresses IP des sites Web d'hameçonnage connus et signale les sites suspects à l'utilisateur. https://fr.barracuda.com/products/sentinel/editions#



COMBATTRE LES MALWARE

- Plusieurs entreprises réputées sont spécialisées dans la sécurité, comme **Bitdefender, McAfee, Symantec et Kaspersky**.
- Elles offrent **une protection complète contre les programmes malveillants** pour les ordinateurs et les appareils mobiles.
- Méfiez-vous des **faux programmes antivirus** qui peuvent s'afficher pendant la navigation sur Internet. La plupart de ces faux programmes antivirus s'affichent dans une publicité ou dans une fenêtre contextuelle qui se présente comme une vraie fenêtre d'avertissement de Windows,.
- Leur contenu indique en général que l'ordinateur est contaminé et qu'il doit être nettoyé. Si vous cliquez n'importe où dans cette fenêtre, vous risquez de télécharger et d'installer un programme malveillant.
- Cliquez ici pour consulter un blog sur les faux programmes antivirus **(Rogue Antivirus):**

  https://zvelo.com/introduction-to-rogue-antivirus/